10/512403

PC[redacted]03/00332

PATENTTI- JA REKISTERIHALLITU[redacted]
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 4.7.2003

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija
Applicant

Mediweb Oy
Vantaa

Patenttihakemus nro
Patent application no

20020808

Tekemispäivä
Filing date

29.04.2002

Kansainvälinen luokka
International class

G06F

Keksinnön nimitys
Title of invention

"Arkaluontoisten tietojen tallentaminen"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Marketta Tehikoski
Apulaistarkastaja

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Arkaluontoisten tietojen tallentaminen

Keksinnön ala

Keksintö liittyy henkilöön liittyvien arkaluontoisten tietojen tallentamiseen ja erityisesti potilaan resepti- ja/tai muiden potilastietojen tallentamiseen.

Keksinnön tausta

Perinteisesti reseptitietoja ei ole tallennettu muualle kuin varsinaiseen paperireseptiin ja mahdollisesti lääkärin käyttämän, suljetun tietojärjestelmän tietokantoihin. Vastaavasti potilastietoja on ylläpidetty paperille tallennettuna ns. potilaskansioihin ja sen lisäksi mahdollisesti lääkäriaseman, terveysaseman ja/tai sairaalan suljetussa tietojärjestelmässä. Ulkopuoliset organisaatiot eivät ole päässeet näihin tietoihin käsiksi. Tietoliikenneyhteyksien parantuessa on kehitetty esimerkiksi erilaisia reseptinvälitysjärjestelmiä, joista useimmat perustuvat siihen, että resepti on lähetetty suoraan lääkkeen toimittavaan apteekkiin, eikä resepteistä näin ollen ole kerätty mitään tietokantaa. Tällaisten ratkaisujen ongelma on kuitenkin ollut se, että henkilön on päätettävä jo reseptin kirjoitusvaiheessa apteekki, jossa aikoo asioida.

Tämän ongelman ratkaisuksi on esitetty keskitettyä tietokantaa, johon reseptit voidaan tallentaa ja josta ne voidaan hakea mistä tahansa apteekista. Tällaisen tietokannan ongelmana on se, että on taattava tietojen luottamuksellisuus eli se, että ulkopuoliset eivät voi saada tietoonsa minkälaisia reseptejä tietylle henkilölle on kirjoitettu.

Eräs tapa ratkaista tämä ongelma on se, että reseptitieto tallennetaan yhdessä henkilöön liittyvän ulkoisen tunnisteen kanssa, josta tunnisteesta ei kuitenkaan pystytä identifioimaan henkilöä, ja tietoon pääsee käsiksi vain mainitulla ulkoisella tunnisteella. Ulkoinen tunniste voi olla esimerkiksi biometrinen tunniste, kuten sormenjälki, tai henkilökohtaisessa älykortissa oleva koodi. Ulkoisen tunnisteen käyttö edellyttää kuitenkin koodinlukijoita sekä tallennuspäässä että tiedonhakupäässä ja jopa sitä, että henkilö kantaa mukanaan koodia erillisessä kortissa tai vastaavassa.

Eräs toinen tapa on suojata tiedot vahvaa salausta käyttäen. Vahvan salauksen ongelmana on, että se vanhenee ajan myötä muuttuen näin turvattomaksi. Resepti- ja potilastietojen tulisi pysyä salaisina useita kymmeniä vuosia. Salaaminen edellyttää myös salausohjelmien käyttöä tietoja tallennettaessa ja salauksen purkuohjelman käyttöä tietoja purettaessa. Nämä ohjelmat

ovat eri salausmenetelmillä erilaisia. Menetelmien haittana on myös se, että niissä tulee sopia siitä, miten salausavaimia käytetään, säilytetään ja vaihdetaan. Lisäksi vahvasti salatun tiedon käyttö tutkimukseen ja muuhun vastaavaan käyttöön on erittäin vaikeaa ja julkisen avaimen salausta käytettäessä käytännössä mahdotonta.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten kehittää menetelmä ja menetelmän toteuttava laitteisto siten, että arkaluontoisia tietoja voidaan hakea henkilöittäin yleisesti käytössä olevalla henkilön tunnisteella, kuten henkilötunnuksella, mutta arkaluontoiset tiedot ovat tallennettu siten, että niitä ei pystytä yhdistämään kehenkään henkilöön. Keksinnön tavoite saavutetaan menetelmällä, tietoliikennepalvelimilla, verkkosolmulla ja järjestelmällä , joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen, että tallennusvaiheessa arkaluontoiset tiedot, kuten reseptin sisältämä lääkemääräys, ja henkilön tunnistetiedot, kuten henkilötunnus, erotetaan toisistaan tallentamalla henkilön tunnistetiedot ensimmäiseen tietokantaan ja arkaluontoiset tiedot toiseen tietokantaan siten, että tiedot sidotaan toisiinsa toisen tunnisteen avulla. Toinen tunniste itsessään ei sisällä mitään, mikä yhdistäisi sen johonkin tiettyyn henkilöön. Näin arkaluontoiset tiedot ovat tarvittaessa haettavissa henkilön tunnistetietojen avulla ja samalla tutkittavissa ilman henkilön tunnistetietoja. Tässä lääkemääräys sisältää edullisesti kaikki reseptissä olevat lääkitystiedot. Toisin sanoen keksintö perustuu kahden erillisen tietokannan käyttöön sisäisen tunnisteen avulla.

Keksinnön etuna on, että arkaluonteisia tietoja ei tarvitse salata, sillä arkaluontoisia tietoja sisältävässä toisessa tietokannassa ei ole mitään, mikä paljastaisi tietoja luvallisesti tai luvattomasti tutkivalle, keneen arkaluontoiset tiedot liittyvät. Lisäksi arkaluontoiset tiedot ovat tutkijoiden ja viranomaisten käytössä ilman, että kenenkään tietosuojaa vaarannetaan ja/tai ilman, että tutkijoille tai viranomaisille pitäisi antaa salaista tietoa, jonka avulla tiedot saisi purettua käyttökelpoiseen muotoon. Lisäksi etuna on se, että tietoja tallennettaessa tai haettaessa tiettyyn henkilöön liittyviä tietoja, järjestelmän käyttäjällä ei tarvitse olla erillisiä lukulaitteita tai vastaavia eikä henkilön tarvitse kantaa mukanaan tai ostaa ylimääräistä tietoa sisältävää tunnistusyksikköä, kuten älykorttia. Vielä eräänä etuna on, että koska tiedonhaussa käytettävä tunniste on

järjestelmän sisäinen tunniste, ei järjestelmän loppukäyttäjien tarvitse huolehtia tietoturvajärjestelmän toiminnasta.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 esittää esimerkkisuoritusmuodon yksinkertaistettua järjestelmäarkkitehtuuria;

Kuvio 2 esittää lohkokaavion verkkosolmusta, joka käsittää esimerkkisuoritusmuodon mukaisen tunnistetietokannan;

Kuvio 3 esittää lohkokaavion verkkosolmusta, joka käsittää esimerkkisuoritusmuodon mukaisen arkaluontoista tietoa sisältävän tietokannan;

Kuvio 4 esittää lohkokaavion esimerkkisuoritusmuodon mukaisesta tietoliikennepalvelimesta;

Kuvio 5 on vuokaavio esimerkkisuoritusmuodon mukaisen tunnistetietokannan käsittävän verkkosolmun toiminnasta;

Kuvio 6 on esimerkkisuoritusmuodon mukaisen arkaluontoista tietoa sisältävän tietokannan käsittävän verkkosolmun toimintaa havainnollistava vuokaavio; ja

Kuvio 7 on esimerkkisuoritusmuodon mukaisen tietoliikennepalvelimen toimintaa havainnollistava vuokaavio.

Keksinnön yksityiskohtainen selostus

Keksintöä tullaan seuraavassa selostamaan käyttäen esimerkkinä reseptin välittämistä reseptitietokannan välityksellä reseptin kirjoittamispisteestä, kuten terveysasemalta tai yksityiseltä lääkäriasemalta, apteekkiin. Keksintöä ei kuitenkaan ole rajoitettu tähän nimenomaiseen ratkaisuun, vaan esillä olevaa keksintöä voidaan soveltaa minkä tahansa arkaluonteisen tiedon, kuten potilashistorian, lääkityshistorian jne, tallentamiseen ja tarvittaessa välittämiseen minne tahansa. Eräs toinen esimerkki, jossa keksintöä voidaan soveltaa, on yhteisen potilashistorian luominen sekä terveysaseman tiedoista että yksityisen lääkäriaseman tiedoista, ja yhteisen potilashistorian käyttö joko terveysasemalta tai yksityiseltä lääkäriasemalta. Keksintöä voidaan myös soveltaa esimerkiksi Internet-kaupankäynnissä laskutus- ja/tai ostotietojen tallentamiseen.

Kuvio 1 esittää yksinkertaistetun järjestelmäarkkitehtuurin kuvaten vain ne elementit, joita tarvitaan keksinnön esimerkkisuoritusmuodon kuvaami-

seen. Kuviossa 1 esitetyt verkkosolmut ovat loogisia yksiköitä, joiden implementaatio voi poiketa esitetystä. Alan ammattilaiselle on ilmeistä että järjestelmä voi käsittää myös muita toimintoja ja rakenteita, joita ei tarvitse kuvata tarkemmin tässä.

Järjestelmä käsittää terveysasemajärjestelmän 1, apteekin järjestelmän 2, sekä kaksi verkkosolmua 3, 4, jotka kumpikin sisältävät tietokannat sekä kaksi tietoliikenneverkkoa 5, 5' joiden välityksellä verkkosolmut 3, 4 ovat kytkettynä terveysasemajärjestelmään 1 ja apteekin järjestelmään 2. Järjestelmässä voidaan käyttää langatonta tiedonsiirtoa, kiinteään yhteyteen perustuvaa tiedonsiirtoa tai molempia.

Kuvion 1 esimerkkisuoritusmuodossa terveysasemajärjestelmä 1 käsittää ainakin reseptintallennusosion 11 ja tietoliikennepalvelimen 12. Reseptintallennusosiolla 11 tarkoitetaan niitä välineitä ja käyttöliittymää UI, joiden avulla resepti voidaan luoda ja välittää tietoliikennepalvelimen 12 välityksellä reseptejä sisältävään tietokantaan. Esimerkkisuoritusmuodon mukaista tietoliikennepalvelinta kuvataan tarkemmin kuvioiden 4 ja 7 yhteydessä.

Kuvion 1 esimerkkisuoritusmuodossa apteekin järjestelmä 2 käsittää tietoliikennepalvelimen 22, jonka avulla resepti haetaan reseptejä sisältävästä tietokannasta ja jonka välityksellä reseptiin mahdollisesti tehtäviä merkintöjä, voidaan tallentaa, sekä reseptin käsittelyosion 21, joka on järjestetty näyttämään reseptin sisällön käyttöliittymän UI' välityksellä apteekin henkilöstölle ja jonka välityksellä henkilöstö voi esimerkiksi tallentaa reseptin toimittamiseen liittyviä tietoja. Esimerkkisuoritusmuodossa apteekin järjestelmässä oleva tietoliikennepalvelin 22 on samanlainen kuin terveysasemajärjestelmässä oleva tietoliikennepalvelin 12. Keksinnön joissain muissa suoritusmuodoissa tietoliikennepalvelimet voivat erota toiminnoiltaan toisistaan.

Alan ammattilaiselle on ilmeistä, että sekä terveysasemajärjestelmä 1 että apteekkijärjestelmä 2 käsittävät muitakin osajärjestelmiä ja/tai osioita, joita ei ole kuvattu tässä tarkemmin, koska ne ovat varsinaisen keksinnön kannalta epäoleellisia. Esimerkkejä tällaisista ovat erilaiset tunnistamisjärjestelmät, ja palomuurit, joilla varmennetaan mm. se, että tietoja pääsee tallentamaan/lukemaan vain sellainen, joka on siihen oikeutettu. Alan ammattilaiselle on myös ilmeistä, että terveysasema- ja/tai apteekkijärjestelmiä ja/tai niiden sisältämiä elementtejä voi olla useita.

Kuvion 1 esimerkkisuoritusmuoto käsittää kaksi erillistä verkkosolmua 3, 4, jotka kumpikin käsittävät tietokannan DB1, DB2. Tietokannat eroa-

vat toisistaan siten, että toiseen tietokantaan on tallennettu arkaluontoisia tietoja eli keksinnön esimerkkisuoritusmuodossa lääkemääräyksiä ja toiseen henkilön yksilöiviä tietoja. Tietokantojen rakennetta kuvataan yksityiskohtaisemmin kuvioiden 2 ja 3 yhteydessä ja niiden toimintaa esimerkkisuoritusmuodossa kuvioiden 5 ja 6 yhteydessä. Keksinnön jossain muussa suoritusmuodossa tietokannat voivat fyysisesti sijaita samassa verkkosolmussa ollen kuitenkin erillisiä tietokantoja. Tietokannat tai toinen niistä voivat käsittää useampia toisiinsa linkitettyjä tietokantoja, jotka voivat sijaita fyysisestikin eri verkkosolmuissa, jotka verkkosolmut voivat olla osa suljettua tai avointa tietoverkkoa. Toisiinsa linkitetyt tietokannat voivat sisältää myös erilaista tietoa. Esimerkiksi avoin tietokanta voi käsittää toisiinsa linkitettyjä tietokantoja siten, että yhdessä linkitetyssä tietokannassa on lääkemääräystietoja, toisessa laboratoriotietoja ja kolmannessa ikä-, pituus- ja painotietoja. Loppukäyttäjälle nämä toisiinsa linkitetyt tietokannat käyttäytyvät kuin yksi yhtenäinen tietokanta.

Kumpikin tietokannan sisältävä verkkosolmu on kytketty tietoliikennepalvelimiin 12, 22 verkkojen 5, 5' välityksellä. Sillä, mihin tietoliikennejärjestelmään välissä olevat verkot perustuvat ja sillä, perustuvatko ne samoihin vai eri järjestelmiin, ei ole keksinnön kannalta merkitystä. Verkot voivat olla esimerkiksi Internet-verkkoja, puhelinverkkoja tai matkaviestinverkkoja.

Vaikka keksinnön esimerkkisuoritusmuodossa oletetaan, että tietoliikennepalvelin on osa sitä osajärjestelmää, jolle se välittää tietoja tietokannasta tai josta se välittää tietoja tietokantaan, on alan ammattilaiselle ilmeistä, että tietoliikennepalvelin voi olla järjestetty omaksi erilliseksi verkkosolmuksi tai jommankumman tietokannan sisältävään solmuun. Sillä, että tietoliikennepalvelin on osa osajärjestelmää, saavutetaan se etu, että yleisessä verkossa ei tarvitse lähettää arkaluontoista tietoa yhdessä henkilötunnuksen kanssa. Näin parannetaan edelleen yksittäisen henkilön tietoturvaa.

Kuviossa 2 havainnollistetaan tunnisteita sisältävää tietokantaa, ns. tunnistetietokantaa eli esimerkkisuoritusmuodon mukaista verkkosolmua 3, joka käsittää yhteysosan 31, sovellusosan 32 ja henkilökohtaista tietoa sisältävän tietokannan DB1.

Henkilökohtaista tietoa sisältävä tietokanta DB1 käsittää tietueita 33, joissa on yhdistetty henkilötunnus HETU tälle nimenomaiselle henkilötunnukselle generoituun tunnisteeseen TUNNISTE. Henkilötunnus on tunniste, jota käytetään henkilön identifioimiseen yksikäsitteisesti. Generoitu tunniste on edullisesti yksikäsitteinen arkaluontoista tietoa sisältävän tietokannan sisällä

siten, että arkaluontoista tietoa sisältävässä tietokannassa yksi generoidun tunnisteen arvo voi liittyä vain yhteen henkilöön. Yhdellä henkilöllä voi olla useita generoituja tunnisteita, mutta esimerkkisuoritusmuodossa oletetaan, että yhdellä henkilöllä on vain yksi generoitu tunniste. Tietokanta voi myös käsittää esimerkiksi listauksena (ei esitetty kuviossa 2) tiedon niistä tietoliikennepalvelimista, joilla on käyttöoikeus tietokannan tietoihin.

Yhteysosa 31 vastaanottaa erilaisia pyyntöjä sekä apteekkijärjestelmän tietoliikennepalvelimelta että terveysasemajärjestelmän tietoliikennepalvelimelta ja välittää vastauksia pyyntöihin. Pyynnöt ovat tyypillisesti tiedonhakupyyntöjä, joilla kysytään tiettyyn henkilötunnukseen liittyvää generoitua tunnistetta. Yhteysosa 31 voi olla myös sovitettu välittämään sovellusosalle 32 tiedon siitä, miltä tietoliikennepalvelimelta pyyntö vastaanotettiin.

Sovellusosa 32 on konfiguroitu etsimään tietokannasta henkilötunnusta vastaavan generoidun tunnisteen ja palauttamaan sen yhteysosan 31 välityksellä sitä kysyneelle tietoliikennepalvelimelle. Lisäksi sovellusosa 32 voi olla konfiguroitu tarkistamaan ennen generoidun tunnisteen hakemista tietokannasta, onko tietoa pyytävä tietoliikennepalvelin sallittu tietoliikennepalvelin, toisin sanoen, löytyykö se esimerkiksi tietokannassa DB1 olevalta listalta, ja jos tietoliikennepalvelin ei ole sallittu, joko esimerkiksi lähettämään pelkän tyhjän tiedon tai negatiivisen kuittauksen tietoa kysyneelle tietoliikennepalvelimelle. Lisäksi sovellusosa 32 voi olla konfiguroitu lisäämään tietokantaan sallittujen tietoliikennepalvelimien listalle uusia tietoliikennepalvelimia. Keksinnön esimerkkisuoritusmuodossa sovellusosa 32 on konfiguroitu silloin, kun generoitua tunnistetta ei löytynyt, lähettämään negatiivisen kuittauksen generoitua tunnistetta kysyneelle tietoliikennepalvelimelle ja vasteena tietoliikennepalvelimelta vastaanotetulle generointipyynnölle generoimaan tunnisteen, tallentamaan sen yhdessä henkilötunnuksen kanssa tietueeksi 33 tietokantaan DB1 ja lähettämään näin generoimansa tunnisteen yhteysosan 31 välityksellä generointipyynnön lähettäneelle tietoliikennepalvelimelle. Generoitu tunniste voi olla esimerkiksi juokseva numero. Keksintö ei kuitenkaan rajoita generoidun tunnisteen muotoa ja/tai sisältöä mitenkään. Keksinnön jossain muissa suoritusmuodoissa, jossa esimerkiksi tietoliikennepalvelin tai joku muu taho huolehtii generoidun tunnisteen generoinnista, sovellusosa 32 on konfiguroitu silloin, kun generoitua tunnistetta ei löytynyt, joko esimerkiksi lähettämään pelkän tyhjän tiedon tai negatiivisen kuittauksen generoitua tunnistetta kysyneelle tietoliikennepalvelimelle. Vielä eräässä keksinnön suoritusmuodossa sovellusosa voi olla

konfiguroitu generoimaan vasteena sille, että henkilötunnukselle ei löydy generoitua tunnistetta, generoidun tunnisteen, tallentamaan sen yhdessä henkilötunnuksen kanssa tietueeksi tietokantaan DB1 ja lähettämään näin generoimansa tunnisteen yhteysosan 31 välityksellä sitä kysyneelle tietoliikennepalvelimelle

Koska esimerkkisuoritusmuodossa vain tunnistetietokanta osaa yhdistää tietyn generoidun tunnisteen tiettyyn henkilöön, pysyvät arkaluontoiset tiedot salaisina toisessa tietokannassa taaten näin henkilön tietoturvan.

Keksinnön jossain muussa suoritusmuodossa tunnistetietokanta voi sisältää henkilötunnuksen lisäksi myös muita vähemmän yksilöiviä tietoja, kuten esimerkiksi osoitteen tai muita demografisia tietoja.

Keksinnön jossain muussa suoritusmuodossa tunnistetietokanta voi myös käsittää suostumuksenhallintaan liittyviä tietoja. Tällaisessa suoritusmuodossa esimerkiksi potilaalta kysytään suostumusta siihen, saako hänen lääkemääräystään/lääkemääräyksiään tallentaa tietokantaan ja/tai minkälaisia tietoja saa tallentaa tietokantaan.

Keksinnön jossain muussa suoritusmuodossa tunnistetietokanta voi lisäksi käsittää alitunnisteita, joita voidaan käyttää sen määrittelemiseen, minkälaisia oikeuksia alitunnisteen omaavalla on käsitellä arkaluontoisia tietoja sisältävän tietokannan tietoja. Eräs esimerkki alitunnisteesta on mainostajan tunniste. Niiden tunnisteiden, joihin mainostajan tunniste on liitetty, omistajille voidaan lähettää mainostajan mainoksia.

Keksinnön muissa suoritusmuodoissa sovellusosa 32 on konfiguroitu suorittamaan suoritusmuotoihin liittyviä toimintoja.

Kuviossa 3 havainnollistetaan arkaluontoisia tietoja sisältävää tietokantaa eli esimerkkisuoritusmuodon mukaista verkkosolmua 4, joka käsittää yhteysosan 41, sovellusosan 42 ja reseptitietokannan DB2.

Yhteysosa 41 vastaanottaa erilaisia pyyntöjä sekä apteekkijärjestelmän tietoliikennepalvelimelta että terveysasemajärjestelmän tietoliikennepalvelimelta ja välittää vastauksia tai kuittauksia pyyntöihin. Pyynnöt ovat tyypillisesti joko tiedonhakupyyntöjä, tiedon tallennuspyyntöjä tai tiedon muokkauspyyntöjä. Yhteysosa 41 voi olla myös sovitettu välittämään sovellusosalle 42 tiedon siitä, miltä tietoliikennepalvelimelta pyyntö vastaanotettiin.

Reseptejä sisältävä tietokanta DB2 käsittää tietueita 43, joissa generoituun tunnisteeseen TUNNISTE on yhdistetty esimerkkisuoritusmuodossa kaikki lääkemääräykset ja muut mahdolliset tunnisteeseen liittyvät tiedot. Toi-

sin sanoen tietoja tallennettaessa etsitään tietue, jossa on vastaava tunniste ja tallennetaan tieto/tiedot siihen siellä jo olevien tietojen lisäksi. Keksinnön jossain muussa suoritusmuodossa tiedot tallennetaan pienempiin tietueisiin, jotka käsittävät tunnisteen ja sillä kerralla tallennetun tiedon. Tässä suoritusmuodossa tietoja haettaessa haetaan tietokannasta kaikki tietueet, joissa on ko. tunniste. Yksinkertaisimmillaan reseptejä sisältävä tietokanta käsittää vain avoimia reseptejä eli reseptejä, joita ei vielä ole toimitettu tai joista osa on toimitettu. Reseptejä sisältävä tietokanta voi käsittää myös esimerkiksi ns. lääkityshistorian, potilashistorian, erilaisia potilaan taustatietoja, kuten ikä, paino, tupakointi, jne, lääkityksen haittavaikutustietoa, laboratoriokokeiden tuloksia ja/tai tietoa allergioista. Tietokanta voi myös käsittää esimerkiksi listauksena (ei esitetty kuviossa 3) tiedon niistä tietoliikennepalvelimista, joilla on käyttöoikeus tietokannan tietoihin. Tietoliikennepalvelimet voivat olla myös listattu siten, että joillakin on oikeus saada vain pyydettyyn tunnisteeseen liittyvää tietoa, joillain on oikeus vain pyyntöihin, joissa ei esiinny tunnistetta (eli massatietoihin) ja joillain tietoliikennepalvelimilla on oikeus kaikkiin tietoihin. Tietokanta voi lisäksi käsittää alitunnisteita, joita voidaan käyttää esimerkiksi sen määrittelemiseen, minkälaisia oikeuksia alitunnisteen omaavalla on käsitellä tietokannan tietoja.

Sovellusosa 42 on konfiguroitu erottamaan toisistaan erilaiset pyynnöt ja toimimaan niiden mukaisesti. Sovellusosa 42 on siten konfiguroitu etsimään tietokannasta generoitua tunnistetta vastaavat lääkemääräykset ja palauttamaan ne yhteysosan 41 välityksellä niitä pyytäneelle tietoliikennepalvelimelle, tallentamaan generoidun tunnisteen yhteyteen uusia lääkemääräyksiä ja muokkaamaan tietokannassa olevia lääkemääräyksiä. Lisäksi sovellusosa 42 voi olla konfiguroitu tarkistamaan ennen avoimien reseptien hakemista, muokkaamista ja/tai tallentamista tietokannasta, onko tietoa pyytävä tietoliikennepalvelin sallittu tietoliikennepalvelin, toisin sanoen, löytyykö se esimerkiksi tietokannassa DB2 olevalta listalta, jolle tällaista tietoa saa antaa, ja jos tietoliikennepalvelin ei ole sallittu, joko esimerkiksi lähettämään pelkän tyhjän tiedon tai negatiivisen kuittauksen pyynnön esittäneelle tietoliikennepalvelimelle. Lisäksi sovellusosa 42 voi olla konfiguroitu lisäämään tietokantaan sallittujen tietoliikennepalvelimien listalle uusia tietoliikennepalvelimia. Sovellusosa 42 voi olla myös konfiguroitu generoimaan ja/tai tallentamaan alitunnisteita. Keksinnön esimerkkisuoritusmuodossa sovellusosa 42 on lisäksi konfiguroitu suorittamaan erilaisia tietokantahakuja. Tietokannasta voidaan hauilla selvittää esimerkiksi, kuinka monta reseptiä (lääkemääräystä) määrättiin viime kuussa ko-

ko maassa tai Helsingissä, mikä on ollut eniten määrätty lääkeyhdistelmä reuman hoitamiseen viimeisten 10 vuoden aikana, montako reseptiä potilaalle A on määrätty viimeisen 3 vuoden aikana tai "Kuinka suuressa %-osuudessa viime vuonna määrätyistä resepteistä määrättiin lääkettä X. Sovellusosa 42 voi olla lisäksi sovitettu generoimaan alitunnisteita.

Kuviossa 4 esitetään lohkokaavio keksinnön esimerkkisuoritusmuodon mukaisesta tietoliikennepalvelimesta 12. Tietoliikennepalvelin voi olla oma, erillinen palvelin tai sitten esimerkiksi järjestelmään liitettävä ohjelmistomoduuli. Keksinnön esimerkkisuoritusmuodossa oletetaan, että järjestelmässä käytetään vain yhden tyyppisiä tietoliikennepalvelimia, jotka lisätään kuhunkin keksinnön mukaisia tietokantoja käyttäviin osajärjestelmiin. Toisin sanoen esimerkkisuoritusmuodossa kaikkiin osajärjestelmiin, jotka hakevat tietoa ja/tai tallentavat tietoa tietokantaan, lisätään saman tyyppinen tietoliikennepalvelin. Keksinnön joissain muissa suoritusmuodoissa tietoliikennepalvelimia voidaan räätälöidä suorittamaan vain niitä toimintoja, joita osajärjestelmässä tarvitaan, kuten esimerkiksi massatiedonhakuja suoraan kuvion 3 tietokannasta ilman mitään tunnisteita.

Esimerkkisuoritusmuodossa oletetaan, että osajärjestelmä, jonka osana tietoliikennepalvelin toimii, autentikoi käyttäjät ja tietoliikenneohjeet siten, että tietoliikennepalvelin voi luottaa siihen, että sitä pääsee käyttämään vain siihen valtuutetut henkilöt/laitteet. Keksinnön joissain muissa suoritusmuodoissa tietoliikennepalvelin voi sisältää erilaisia käyttäjien ja/tai laitteiden autentikointitoimintoja ja/tai -välineitä tietoturvasyistä.

Viitaten kuvioon 4 esimerkkisuoritusmuodon mukainen tietoliikennepalvelin 12 käsittää kaksi erillistä yhteysosaa 121, 121' ja niiden välisen sovellusosan 122.

Ensimmäinen yhteysosa 121 on konfiguroitu olemaan yhteydessä siihen osajärjestelmään, jonka osa tietoliikennepalvelin on. Se vastaanottaa käyttäjiltä pyyntöjä ja välittää ne edelleen sovellusosalle sekä vastaanottaa sovellusosalta pyyntöihin tulleet vastaukset ja välittää ne edelleen käyttäjälle käyttöliittymän välityksellä.

Toinen yhteysosa 121' on konfiguroitu olemaan yhteydessä tunnistetietokantaan ja arkaluontoisia tietoja sisältävään tietokantaan eli reseptitietokantaan. Toinen yhteysosa lähettää sovellusosalta vastaanottamiaan tiedonhaku- tai tallennuspyyntöjä tai niiden perusteella generoituja pyyntöjä tietokan-

toja sisältäville verkkosolmuille ja vastaanottaa niiltä vastauksia, jotka se edelleen välittää sovellusosalle.

Esimerkkisuoritusmuodon mukainen sovellusosa 122 on konfiguroitu suorittamaan tarkemmin kuvion 7 yhteydessä suoritettavat toiminnot. Lyhyesti sanottuna sovellusosa 122 on konfiguroitu vasteena henkilötunnuksen sisältävälle pyynnölle selvittämään henkilötunnisteelle generoitu tunniste ja pyynnöstä riippuen joko tallentamaan, muokkaamaan tai hakemaan arkaluontoista tietoa generoidun tunnisteen perusteella. Vastaavasti sovellusosa on konfiguroitu vasteena henkilötunnuksen sisältämättömälle pyynnölle lähettämään pyynnön arkaluontoista tietoa sisältävälle tietokannalle. Lisäksi esimerkkisuoritusmuodon mukainen sovellusosa 122 on konfiguroitu kysymään käyttäjältä, generoidaanko henkilötunnukselle tunniste, silloin kun sitä ei tietokannasta löytynyt ja mikäli käyttäjä niin haluaa, pyytämään tunnisteen generoimista. Keksinnön jossain muussa suoritusmuodossa sovellusosa voi olla konfiguroitu tarkistamaan vasteena henkilötunnuksen sisältävälle pyynnölle pyytäjän oikeus esittää pyyntö ja suorittamaan pyynnön edellyttämät toiminnot vain, jos pyytäjällä on oikeus esittää pyyntö.

Keksinnön jossain muussa suoritusmuodossa tietoliikennepalvelin voi käsittää muistia, johon on allokoitu ennalta määrätty määrä generoituja tunnisteita tai tietty tunnisteavaruus, josta tunnisteita voidaan generoida. Tässä suoritusmuodossa sovellusosa 122 on järjestetty vasteena tunnistetietokannalta vastaanotettuun tyhjään vastaukseen tai negatiiviseen kuittaukseen generoimaan henkilötunnukselle generoidun tunnisteen, käyttämään sitä eteenpäin lähetettävässä pyynnössä ja lähettämään sen tunnistetietokantaan tallennettavaksi, mikäli pyyntö on tiedon tallennuspyyntö. Ennalta määrätyillä tunnisteilla tai tunnisteavaruudella saavutetaan se etu, että ei generoida tunnistetta, jonka joku toinen tietoliikennepalvelin on mahdollisesti generoinut jollekin toiselle henkilötunnukselle.

Keksinnön eräässä toisessa suoritusmuodossa tietoliikennepalvelin voi käsittää paikallisen tunnistetietokannan. Tässä suoritusmuodossa tietoliikennepalvelin on konfiguroitu ensin etsimään generoitua tunnistetta omasta tietokannastaan ja vasta, jos ei löydä sitä, kysymään sitä varsinaiselta tunnistetietokannalta. Tässä suoritusmuodossa tietoliikennepalvelin on myös edullisesti konfiguroitu synkronoimaan paikallisen tunnistetietokantansa joko mahdollisimman usein (esimerkiksi tunnin välein) tai tarvittaessa (aina uuden tunnisteen generoinnin jälkeen) varsinaisen tunnistetietokannan kanssa.

Kuviossa 5 havainnollistetaan esimerkkisuoritusmuodon mukaisen tunnistetietokannan sisältävän verkkosolmun toimintaa vuokaavion avulla. Esimerkkisuoritusmuodossa oletetaan, että tietokanta sisältää myös listauksen niistä tietoliikennepalvelimista, joilla on pääsy tietokannan tietoihin.

Kun verkkosolmu vastaanottaa pyynnön kohdassa 500, se tarkistaa kohdassa 501, oliko pyyntö hakupyyntö. Jos oli, se tarkistaa kohdassa 502, sisälsikö pyyntö henkilötunnusta hetu. Jos pyyntö sisälsi henkilötunnuksen, tarkistaa verkkosolmu kohdassa 503, vastaanotettiinko pyyntö tietoliikennepalvelimelta, jolla on pääsy tietokannan tietoihin. Toisin sanoen tarkistetaan, onko tietoliikennepalvelin sallittu palvelin. Jos on, kohdassa 504 etsitään henkilötunnusta vastaavaa generoitua tunnistetta tunnistetietokannasta. Jos tunniste löytyi tietokannasta (kohta 505), lähetetään se kohdassa 506 vastauksena pyyntöön.

Jos kyseessä ei ollut hakupyyntö (kohta 501), keksinnön esimerkkisuoritusmuodossa on kyseessä tunnisteen generointipyyntö, jonka seurauksena tunniste generoidaan kohdassa 507 ja tallennetaan se kohdassa 508 henkilötunnuksen kanssa tietueeksi tunnistetietokantaan, ja lähetetään kohdassa 506 vastauksena pyyntöön.

Jos pyynnössä ei ollut mukana henkilötunnusta (kohta 502), tai palvelin ei ollut sallittu (kohta 503) tai tunnistetta ei löydetty, (kohta 505), lähetetään negatiivinen kuittaus kohdassa 509.

Kuviossa 6 havainnollistetaan esimerkkisuoritusmuodon mukaisen reseptitietokannan eli arkaluontoisia tietoja sisältävän verkkosolmun toimintaa vuokaavion avulla. Esimerkkisuoritusmuodossa oletetaan, että tietokanta sisältää myös listauksen niistä tietoliikennepalvelimista, joilla on pääsy tietokannan tietoihin siten, että erikseen ei ole listattu niitä tietoliikennepalvelimia, joilla on oikeus hakea generoidun tunnisteen perusteella tietoa ja niitä, joilla sitä oikeutta ei ole. Keksinnön esimerkkisuoritusmuodossa oletetaan, että tiettyyn henkilöön liittyviin tietoihin kohdistuvat pyynnöt erotetaan pyynnössä olevan tunnisteen perusteella massatietopyynnöistä.

Kuvion 6 esimerkissä oletetaan selvyyden vuoksi, että pyydetty tieto löytyy. Alan ammattilaiselle on ilmeistä, että mikäli pyydettyä tietoa ei löydy, pyyntöön vastataan lähettämällä esimerkiksi negatiivinen kuittaus, joka voi sisältää syyn.

Viitaten kuvioon 6, kun verkkosolmu vastaanottaa pyynnön kohdassa 601, se tarkistaa kohdassa 602, vastaanotettiinko pyyntö tietoliikennepalve-

limelta, jolla on pääsy tietokannan tietoihin. Toisin sanoen tarkistetaan, onko tietoliikennepalvelin sallittu palvelin. Jos on, tarkistetaan kohdassa 603, sisälsikö pyyntö tunnisteen. Toisin sanoen tarkistetaan, onko kyseessä jonkin henkilön tietoihin liittyvä pyyntö vai massatietopyyntö. Jos pyynnössä oli tunniste, tarkistetaan kohdassa 604, onko pyyntö tiedon hakupyyntö. Jos on, haetaan kohdassa 605 pyydetty tieto, liitetään kohdassa 606 tieto tunnisteeseen ja lähetetään kohdassa 607 vastaus tietoliikennepalvelimelle.

Jos kyseessä ei ollut hakupyyntö (kohta 604), tarkistetaan kohdassa 608, onko kyseessä tallennuspyyntö. Jos on, tallennetaan kohdassa 609 tietokantaan pyynnössä oleva tieto yhdessä tunnisteen kanssa ja lähetetään kohdassa 610 tietoliikennepalvelimelle positiivinen kuittaus. Esimerkkisuoritusmuodossa kullakin tunnisteella on yksi tietue, johon tieto tallennetaan siellä jo mahdollisesti olevan tiedon lisäksi.

Jos kyseessä ei ollut tallennuspyyntökään (kohta 608), on esimerkkisuoritusmuodossa kyseessä tallennetun tiedon muokkauspyyntö, jolloin kohdassa 611 tallennetaan tunnisteen ja pyynnön yhdessä osoittamaan tietoon halutut muutokset ja lähetetään kohdassa 610 positiivinen kuittaus tietoliikennepalvelimelle.

Jos pyyntö ei sisältänyt tunnistetta (kohta 603), on kyseessä isompaan tietomassaan liittyvä hakupyyntö, joista esimerkkejä on esitetty edellä, ja kohdassa 612 haetaan pyydetty tietomassa tietokannasta ja lähetetään se kohdassa 607 vastauksena tietoliikennepalvelimelle.

Jos kyseessä ei ollut sallittu palvelin (kohta 602), lähetetään tietoliikennepalvelimelle kohdassa 613 negatiivinen kuittaus.

Kuviossa 7 havainnollistetaan esimerkkisuoritusmuodon mukaisen tietoliikennepalvelimen toimintaa. Esimerkkisuoritusmuodossa oletetaan, että yhteyden tietoliikennepalvelimeen pystyy muodostamaan ainoastaan käyttäjä, joka siihen on oikeutettu. Keksinnön jossain muussa suoritusmuodossa tietoliikennepalvelin voi olla konfiguroitu suorittamaan erilaisia autentikointitoimenpiteitä. Esimerkkisuoritusmuodon mukaiseen tunnusmerkkitietokantaan on konfiguroitu niiden verkkosolmujen osoitteet, joissa käytettävät tietokannat sijaitsevat. Lisäksi esimerkkisuoritusmuodossa oletetaan, että generoitavat tunnisteet generoidaan tietokannan sisältävässä verkkosolmussa.

Kun tietoliikennepalvelin vastaanottaa kohdassa 700 käyttäjän pyynnön, se tarkistaa kohdassa 701, sisälsikö pyyntö henkilötunnuksen hetu. Jos sisälsi, tietoliikennepalvelin erottaa kohdassa 702 henkilötunnuksen käyt-

täjän pyynnöstä ja lähettää kohdassa 703 tunnistetietokannan sisältävälle verkkosolmulle hakupyynnön, joka sisältää erotetun henkilötunnuksen.

Jos tunnistetietokannan sisältävältä verkkosolmulta vastaanotettiin kohdassa 704 vastaus, joka sisälsi generoidun tunnisteen (kohta 705), laittaa tietoliikennepalvelin sen käyttäjän pyyntöön kohdassa 706 ja lähettää kohdassa 707 käyttäjän pyynnön reseptitietokannan sisältävälle verkkosolmulle. Lähetettävä käyttäjän pyyntö ei sisällä henkilötunnusta vaan generoidun tunnisteen.

Tietoliikennepalvelin vastaanottaa kohdassa 708 reseptitietokannan sisältävältä verkkosolmulta vastauksen, poistaa kohdassa 709 vastaanottamasta vastauksestaan generoidun tunnisteen, lisää kohdassa 710 henkilötunnuksen vastaukseen ja lähettää kohdassa 711 vastauksen käyttäjälle. Tietoliikennepalvelin toimii näin riippumatta vastauksen sisällöstä. Samalla tietoliikennepalvelin poistaa muististaan sinne väliaikaisesti tallentamansa henkilötunnuksen. Keksinnön jossain muussa edullisessa suoritusmuodossa tietoliikennepalvelin voi kerätä paikallista tunnistetietokantaa, jolloin tallentaa siihen henkilötunnuksen siihen liittyvän generoidun tunnisteen kanssa.

Jos käyttäjän pyyntö ei sisältänyt henkilötunnusta (kohta 701), lähettää tietoliikennepalvelin kohdassa 712 käyttäjän pyynnön reseptitietokannan sisältävälle verkkosolmulle. Vastaanotettuaan kohdassa 713 siltä vastauksen, lähettää tietoliikennepalvelin kohdassa 714 vastauksen käyttäjälle riippumatta vastauksen sisällöstä.

Jos tunnistetietokannalta vastaanotettu vastaus ei sisältänyt tunnistetta (kohta 705), kysyy tietoliikennepalvelin kohdassa 715 käyttäjältä, haluaako hän, että henkilötunnukselle generoidaan tunniste. Jos käyttäjä haluaa (kohta 716), että tunniste generoidaan, lähettää tietoliikennepalvelin tunnistetietokannan sisältävälle verkkosolmulle kohdassa 717 generointipyynnön, johon ottaa vastauksen kohdassa 704, josta jatketaan edellä kuvatulla tavalla.

Jos käyttäjä ei halunnut (kohta 716), että tunnistetta generoidaan, lähettää tietoliikennepalvelin kohdassa 718 käyttäjälle kuittauksen, jossa toteaa, että tieto on vastaanotettu. Samalla tietoliikennepalvelin poistaa muististaan sinne väliaikaisesti tallentamansa henkilötunnuksen.

Keksinnön jossain muussa edullisessa suoritusmuodossa tietoliikennepalvelin ei tallenna edes väliaikaisesti henkilötunnusta ja tässä suoritusmuodossa tietoliikennepalvelin on konfiguroitu kysymään kohtien 709 ja 710 välissä generoidulla tunnisteella henkilötunnusta. Tässä suoritusmuodossa tunnistetietokannan sisältävä verkkosolmu on konfiguroitu palauttamaan tieto-

liikennepalvelimelle henkilötunnuksen vasteena generoidun tunnisteen vastaanotolle.

Kuvioissa 5, 6 ja 7 esitetyt kohdat eivät ole absoluuttisessa aikajärjestyksessa ja ne voidaan suorittaa annetusta järjestyksestä poiketen. Muita toimintoja, kuten käyttäjän autentikointi ja suostumuksenhallintaan liittyvät toimenpiteet, voidaan myös suorittaa kohtien välissä Esimerkiksi tietoliikennepalvelin tai jommankumman tietokannan sisältävä verkkosolmu voi tarkistaa, onko yhteydenottajalla oikeus tietoihin, esimerkiksi onko yhteydenottaja tietty terveyskeskus, tietty lääkäri, sallittu mainostaja tai apteekkari. Osa kuvioissa esitetyistä kohdista, kuten sen tarkistaminen, onko tietoliikennepalvelin sallittu, voidaan jättää myös pois. On myös mahdollista, että tietoliikennepalvelin tunnistaa jo suoraan pyynnöstä, millainen pyyntö on kyseessä, jolloin ei tarvitse tarkistaa, sisälsikö pyyntö henkilötunnuksen tai generoidun tunnisteen. Vastaavasti tunnistetietokannan sisältävä verkkosolmu voi tunnistaa esimerkiksi jo hakupyynnön rakenteesta, onko hakupyyntö sellainen, että mikäli tunnistetta ei löydy, sille voidaan generoida oma tunniste, jolloin kuviossa 5 esitetyt vaiheet muuttavat järjestystä, osa vaiheista voi jäädä pois ja uusia vaiheita voi tulla tilalle.

Vaikka keksintö on selitetty edellä olettaen, että yhteen henkilötunnukseen liittyy ainoastaan yksi generoitu tunniste, on alan ammattilaiselle ilmeistä, että keksintöä voidaan soveltaa myös ratkaisuihin, joissa henkilötunnukseen liittyy useampi generoitu tunniste. Tietokantojen käyttö näissä suoritusmuodoissa on alan ammattilaiselle ilmeistä edellä olevan selityksen perusteella.

Tulisi lisäksi huomata, että edellä tietokantojen käyttöä on esitetty hyvin pelkistetyin esimerkein ja alan ammattilaiselle on ilmeistä, että keksinnön mukaisiin tietokantoihin voidaan toteuttaa keksinnön periaatteita noudattaen hyvinkin monimutkaisia tietokantakyselyjä ja tietojen päivittämisiä. Esimerkiksi lääkityksen numeroinnin muuttuminen voidaan tehdään suoraan massa-ajona arkaluontoisia tietoja sisältävään tietokantaan kaikkiin niihin resepteihin, jotka sisältävät lääkkeen, jonka numerointi muuttuu.

Vaikka edellä on oletettu, että tiedonsiirto ja tallennettava arkaluontoinen tieto on salaamatonta, keksintöä ei ole rajoitettu tällaiseen ratkaisuun. Arkaluontoinen tieto tai osa siitä voidaan tallentaa salattuna. Myös tiedonsiirto tai osa siitä voidaan suorittaa salattuna.

Vaikka keksintöä on edellä selostettu olettaen, että potilaan henkilötiedot turvataan, voidaan keksintöä soveltaa myös reseptin kirjoittaneen lääkärin henkilötietojen turvaamiseen vastaavasti muodostamalla lääkäreiden tunnuksille generoituja tunnisteita ja tallentamalla ne joko omaan tai samaan tunnistetietokantaan.

Vaikka keksintö on edellä selostettu käyttäen henkilötunnusta henkilön identifioivana tunnisteena, on alan ammattilaiselle ilmeistä, että vaihtoehtoisesti tai henkilötunnuksen rinnalla voidaan käyttää muita henkilön riittävällä tarkkuudella identifioivia tunnisteita.

Nykyisen keksinnön toiminnallisuuden toteuttava järjestelmä ja sen verkkosolmut ja järjestelmäosat käsittävät tunnetun tekniikan mukaisten välineiden lisäksi välineitä edellä tarkemmin kuvattujen toimintojen toteuttamiseen. Ne käsittävät prosessoreita ja muistia, joita voidaan hyödyntää keksinnön mukaisissa toiminnoissa. Kaikki keksinnön toteuttamiseen tarvittavat prosessointi- ja muut välineet, muutokset ja lisäykset voidaan suorittaa lisättyinä tai päivitettyinä ohjelmistorutiineina, prosessoreina ja/tai erilaisilla sovelluspiireillä (ASIC).

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.

Patenttivaatimukset

1. Menetelmä arkaluontoisen tiedon tallentamiseksi järjestelmässä, joka käsittää kaksi tietokantaa, joka menetelmä käsittää ainakin vaiheet:

vastaanotetaan tallennuspyyntö, joka käsittää tallennettavan tiedon ja ensimmäisen tunnisteen, joka identifioi henkilön, johon tallennettava tieto liittyy;

t u n n e t t u siitä, että

generoidaan (507) toinen tunniste;

tallennetaan (508) ensimmäiseen tietokantaan ensimmäinen tunniste ja toinen tunniste siten, että ensimmäinen tunniste sidotaan toiseen tunnisteeseen; ja

tallennetaan toiseen tietokantaan tallennettava tieto yhdessä toisen tunnisteen kanssa.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että se käsittää lisäksi vaiheet:

tarkistetaan (505) ennen toisen tunnisteen generoimista ensimmäisestä tietokannasta, onko ensimmäiselle tunnisteelle jo generoitu toinen tunniste;

mikäli on, käytetään ensimmäisessä tietokannassa olevaa toista tunnistetta; ja

mikäli ei ole, generoidaan toinen tunniste.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että se käsittää lisäksi vaiheet:

vastaanotetaan hakupyyntö, joka sisältää ensimmäisen tunnisteen;

haetaan ensimmäisestä tietokannasta ensimmäistä tunnistetta vastaava toinen tunniste; ja

haetaan toisesta tietokannasta pyydetty tieto toista tunnistetta käyttäen.

4. Patenttivaatimuksen 3 mukainen menetelmä, t u n n e t t u siitä, että se käsittää lisäksi vaiheen, jossa lähetetään pyyntöön vastaus, joka sisältää pyydetyn tiedon ja ensimmäisen tunnisteen.

5. Tietoliikennepalvelin (12, 22) tietojärjestelmässä, joka käsittää ainakin kaksi tietokantaa ja tallennettavan tiedon tuottavan järjestelmän, joka tietoliikennepalvelin käsittää

vastaanottovälineet (121) pyynnön vastaanottamiseksi, joka pyyntö sisältää tallennettavan tiedon ja ensimmäisen tunnisteen, joka identifioi henkilön, johon tallennettava tieto liittyy;

t u n n e t t u siitä, että tietoliikennepalvelin (12, 22) käsittää lisäksi

ensimmäiset prosessointivälineet (122) ensimmäistä tunnistetta vastaavan toisen tunnisteen selvittämiseksi tietojärjestelmän ensimmäisestä tietokannasta; ja

toiset prosessointivälineet (122) tallennettavan tiedon tallentamiseksi yhdessä toisen tunnisteen kanssa tietojärjestelmän toiseen tietokantaan.

6. Patenttivaatimuksen 5 mukainen tietoliikennepalvelin (12, 22), t u n n e t t u siitä, että

vastaanottovälineet (121) on sovitettu vastaanottamaan myös tiedonhakupyyntö ja erottamaan sen tallennuspyynnöstä; ja

toiset prosessointivälineet (122) on sovitettu lisäksi hakemaan tallennettu tieto yhdessä toisen tunnisteen kanssa tietojärjestelmän toisesta tietokannasta vasteena tiedonhakupyynnölle ja välittämään haettu tieto ilman toista tunnistetta tiedonhakupyynnön esittäjälle.

7. Tietoliikennepalvelin (12, 22) tietojärjestelmässä, joka käsittää ainakin kaksi tietokantaa ja tallennettua tietoa sisältävän järjestelmän, joka tietoliikennepalvelin käsittää

vastaanottovälineet (121) pyynnön vastaanottamiseksi, joka pyyntö liittyy tallennuttuun tietoon ja sisältää ensimmäisen tunnisteen, joka identifioi henkilön, johon tallennettu tieto liittyy;

t u n n e t t u siitä, että tietoliikennepalvelin käsittää lisäksi

ensimmäiset prosessointivälineet (122) ensimmäistä tunnistetta vastaavan toisen tunnisteen selvittämiseksi tietojärjestelmän ensimmäisestä tietokannasta; ja

toiset prosessointivälineet (122) tallennetun tiedon hakemiseksi yhdessä toisen tunnisteen kanssa tietojärjestelmän toisesta tietokannasta.

8. Verkkosolmu, joka käsittää

tietokannan (DB1) tietojen tallentamiseen, ja

vastaanottovälineet (31) tietokantaan kohdistuvan pyynnön vastaanottamiseksi ja pyynnössä olevan ensimmäisen tunnisteen erottamiseksi, joka ensimmäinen tunniste identifioi henkilön, johon tallennettava tieto liittyy;

t u n n e t t u siitä, että verkkosolmu käsittää lisäksi

generointivälineet (32) toisen tunnisteen generoimiseksi ensimmäiselle tunnisteelle;

tallennusvälineet (32) ensimmäisen tunnisteen ja toisen tunnisteen tallentamiseksi tietokantaan siten, että ensimmäinen tunniste sidotaan toiseen tunnisteeseen; ja

vastausvälineet (31) toisen tunnisteen palauttamiseksi vasteena pyyntöön.

9. Patenttivaatimuksen 8 mukainen verkkosolmu, t u n n e t t u siitä, että

se käsittää lisäksi prosessointivälineet (32) sen tarkistamiseksi, sisältääkö tietokanta ensimmäiselle tunnisteelle toisen tunnisteen, ja mikäli ei löydy, liipaisemaan generointivälineet; ja

generointivälineet (32) on konfiguroitu olemaan vasteellisia prosessointivälineille.

10. Tietojärjestelmä, joka käsittää

ainakin yhden tietoliikennepalvelimen (12, 22)

ainakin kaksi tietokantaa (DB1, DB2)

t u n n e t t u siitä, että

ensimmäinen tietokanta (DB1) käsittää tietueita, joissa henkilön identifoiva ensimmäinen tunniste on liitetty ainakin yhteen toiseen tunnisteen, joka yksinään ei identifoi henkilöä;

toinen tietokanta (DB2) käsittää arkaluontoista tietoa tallennettuna siten, että kukin henkilökohtainen tieto on sidottu vastaavaan toiseen tunnisteeseen; ja

tietoliikennepalvelin (12, 22) on järjestetty vasteena ensimmäisen tunnisteen sisältävälle pyynnölle selvittämään ensimmäistä tunnistetta vastaavan toisen tunnisteen ensimmäisestä tietokannasta, poistamaan pyynnöstä ensimmäisen tunnisteen, lisäämään pyyntöön toisen tunnisteen ja sen jälkeen lähettämään pyynnön toiselle tietokannalle.

(57) Tiivistelmä

Keksinnön kohteena on menetelmä, järjestelmä, tietoliikennepalvelimet ja verkkosolmu arkaluontoisten tietojen tallentamiseen siten, että ne ovat tarvittaessa helposti haettavissa esimerkiksi henkilötunnisteella ilman ylimääräisiä tunnisteita, mutta tallennettu niin, ettei niitä pystytä yhdistämään henkilöön. Keksintö perustuu sisäisen tunnisteen ja kahden erillisen tietokannan käyttöön siten, että kun vastaanotetaan tallennuspyyntö (700), joka käsittää tallennettavan tiedon ja ensimmäisen tunnisteen, joka identifioi henkilön, johon tallennettava tieto liittyy; niin generoidaan toinen tunniste; tallennetaan ensimmäiseen tietokantaan ensimmäinen tunniste ja toinen tunniste siten, että ensimmäinen tunniste sidotaan toiseen tunnisteeseen; ja tallennetaan toiseen tietokantaan tallennettava tieto yhdessä toisen tunnisteen kanssa.

(Kuvio 7)

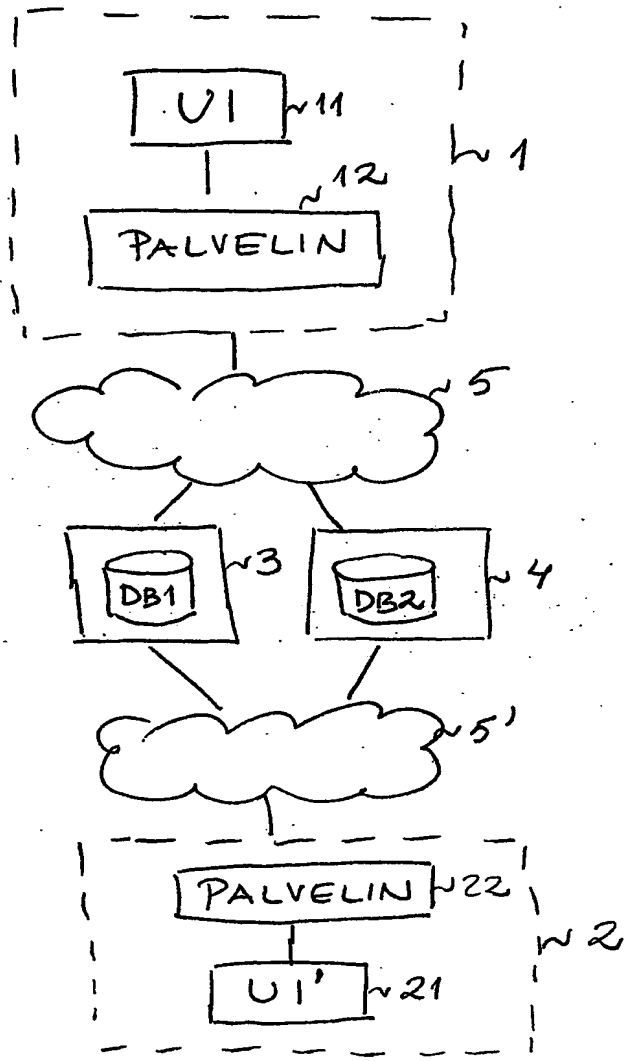
U1
11
12
PALVELIN
1
5
DB1
3
DB2
4
5'
PALVELIN
22
2
U1'
21

FIG 1

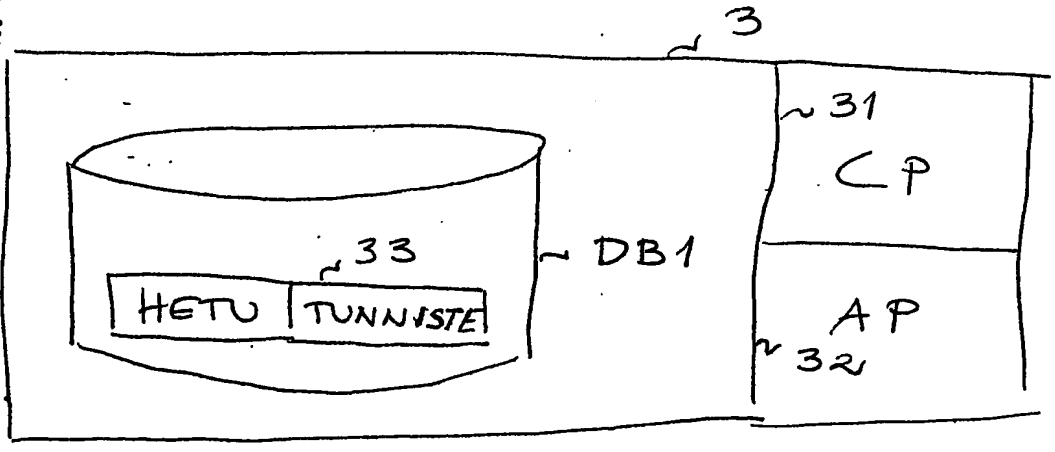
3
31
CP
33
DB1
HETU
TUNNISTE
AP
32

FIG 2

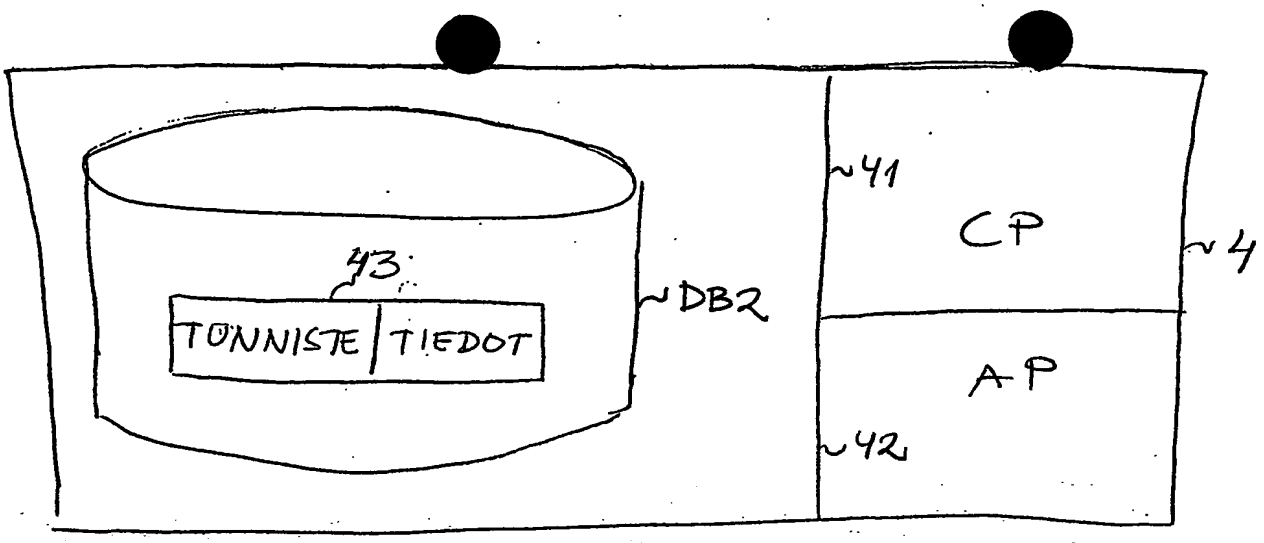

FIG 3

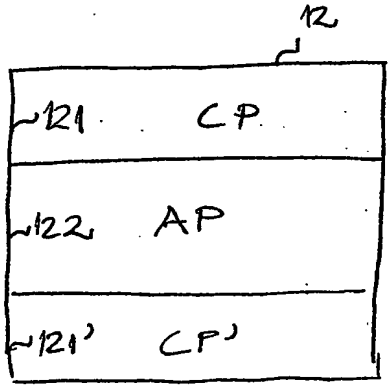

FIG 4

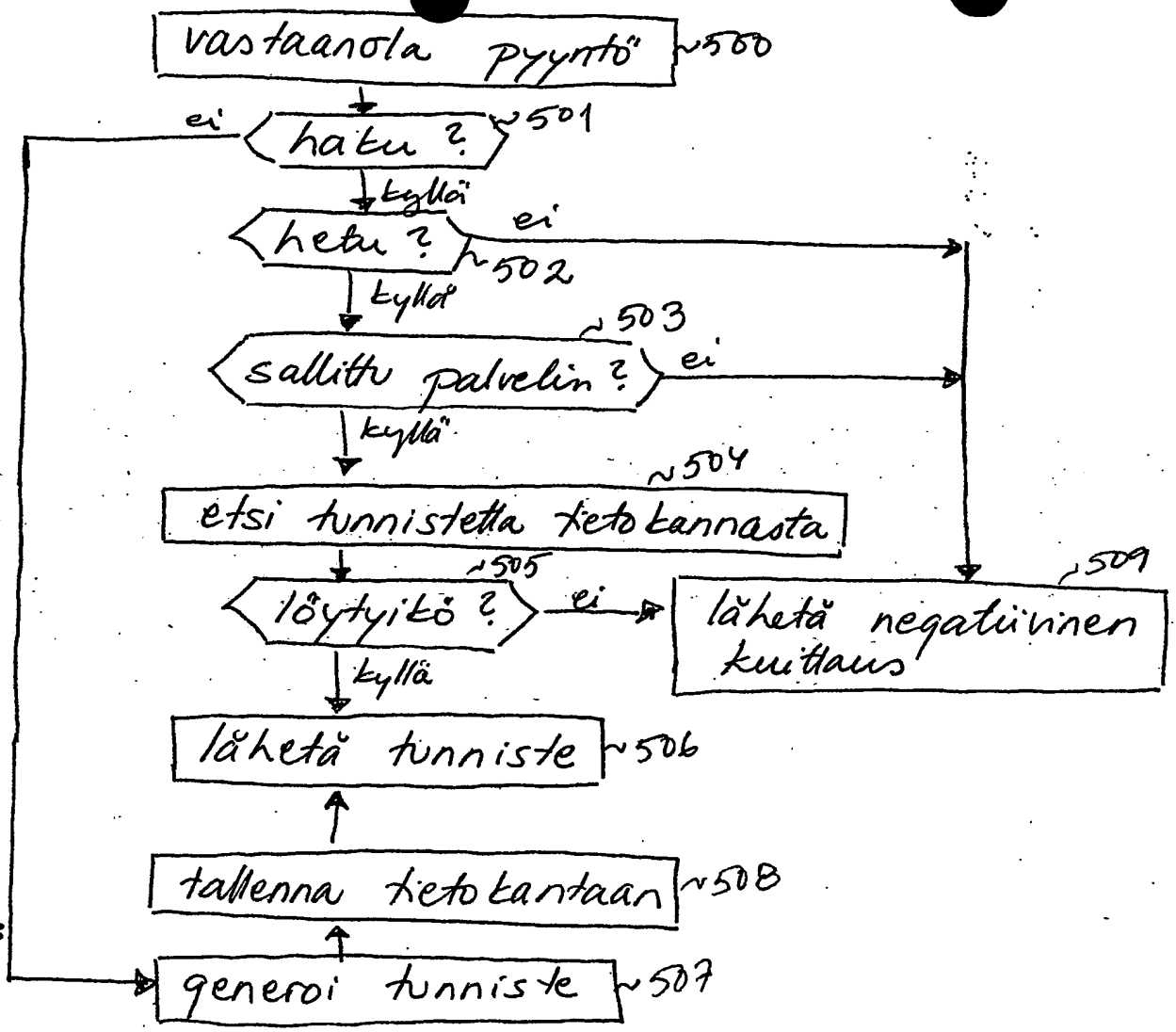
vastaanota pyyntö
500
haku ?
501
ei
kyllä
heti ?
502
ei
kyllä
sallittu palvelin ?
503
ei
kyllä
etsi tunnistetta tietokannasta
504
löytyikö ?
505
ei
kyllä
lähetä negatiivinen kuittaus
509
lähetä tunniste
506
tallenna tietokantaan
508
generoi tunniste
507

FIG 5

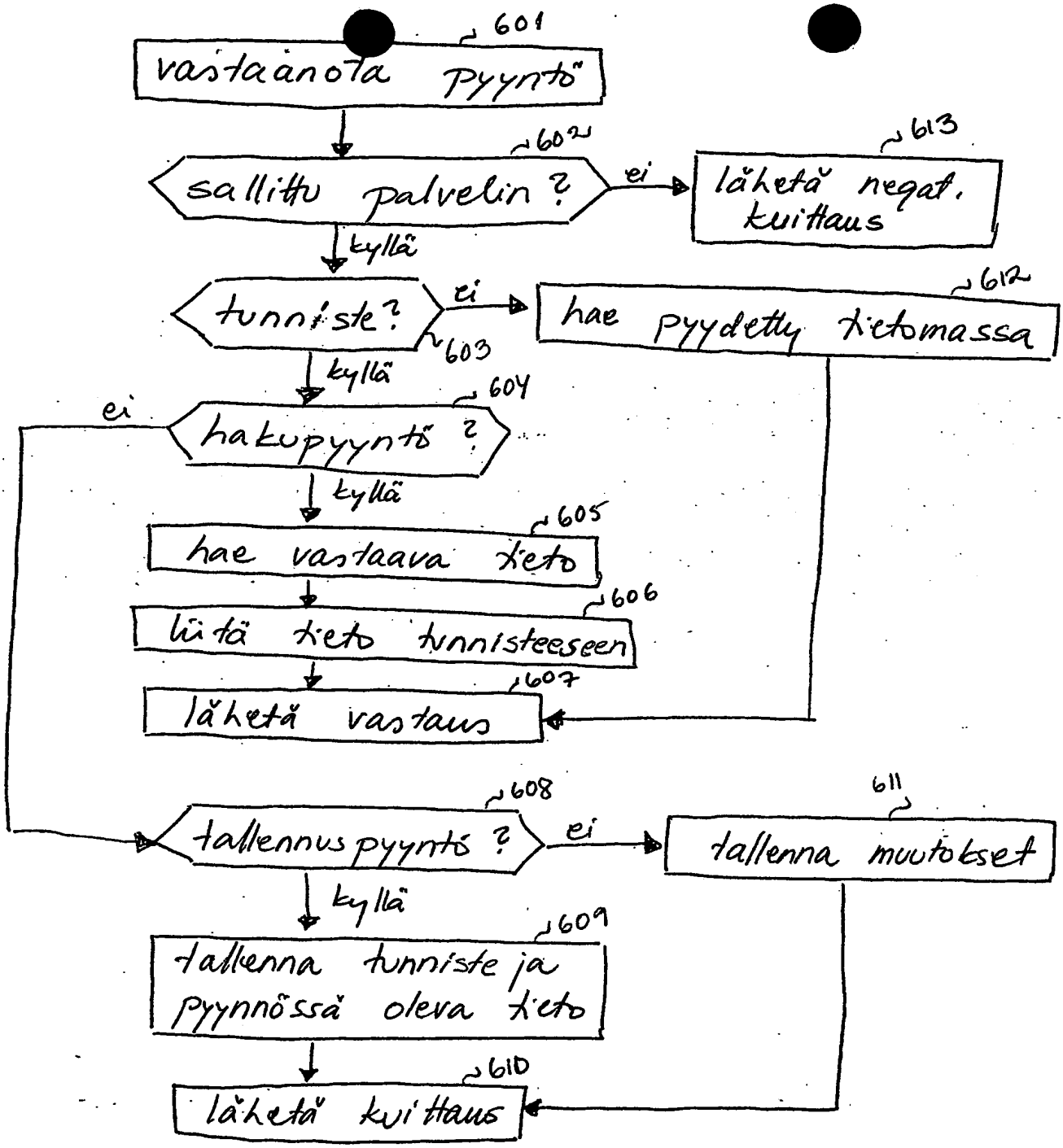
601
vastaanota pyyntö
602
sallittu palvelin ?
ei
613
lähetä negat. kuittaus
kyllä
tunniste?
ei
612
hae pyydetty tietomassa
603
kyllä
604
ei
hakupyyntö ?
kyllä
605
hae vastaava tieto
606
liitä tieto tunnisteeseen
607
lähetä vastaus
608
611
tallennuspyyntö ?
ei
tallenna muutokset
kyllä
609
tallenna tunniste ja pyynnössä oleva tieto
610
lähetä kuittaus

FIG 6

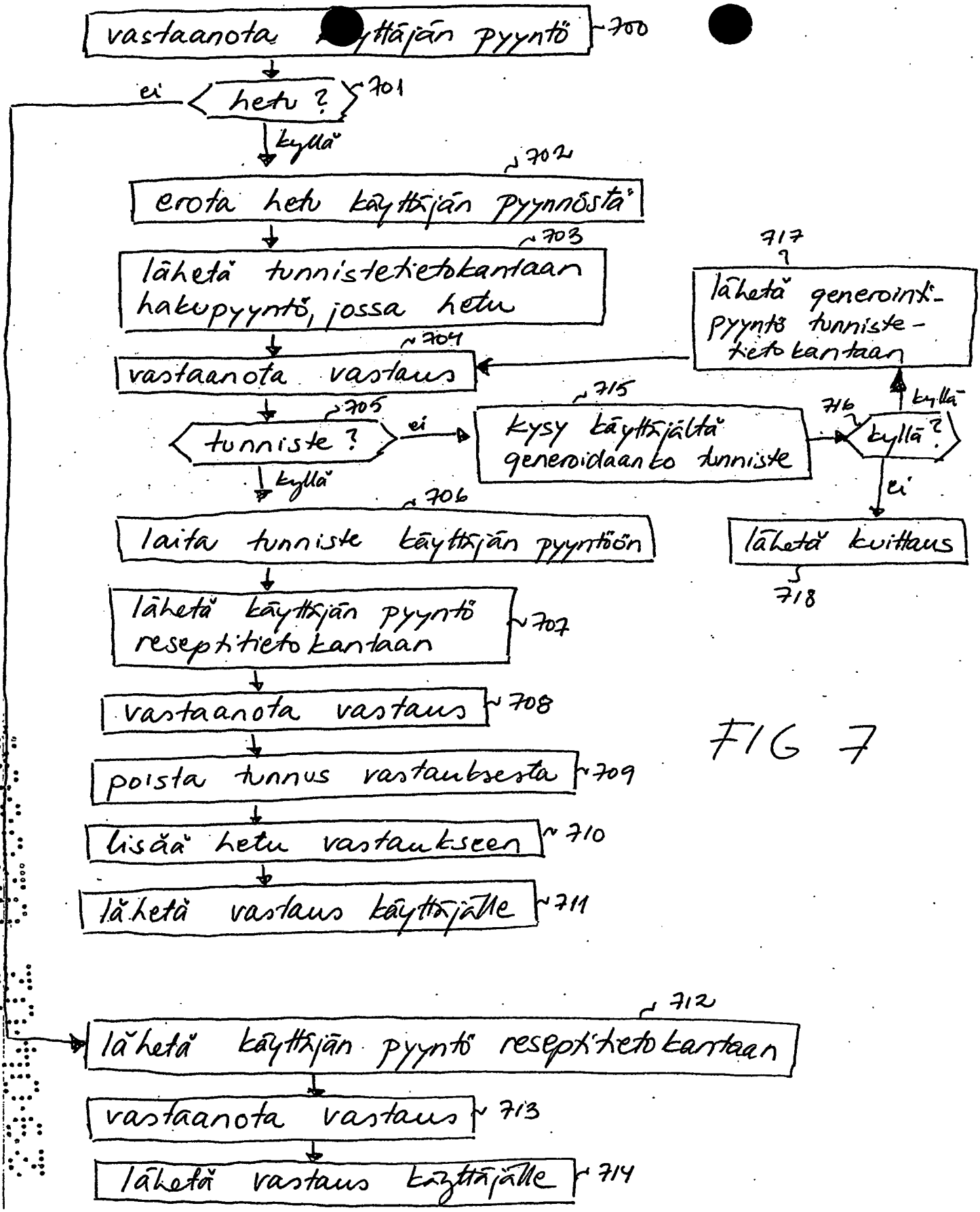
vastaanota käyttäjän pyyntö
700
hetu ?
701
ei
kyllä
erota hetu käyttäjän pyynnöstä
702
lähetä tunnistetietokantaan hakupyyntö, jossa hetu
703
vastaanota vastaus
704
tunniste ?
705
ei
kyllä
laita tunniste käyttäjän pyyntöön
706
lähetä käyttäjän pyyntö reseptitietokantaan
707
vastaanota vastaus
708
poista tunnus vastauksesta
709
lisää hetu vastaukseen
710
lähetä vastaus käyttäjälle
711
kysy käyttäjältä generoidaanko tunniste
715
kyllä ?
716
kyllä
ei
lähetä generointi-pyyntö tunniste-tietokantaan
717
lähetä kuittaus
718
lähetä käyttäjän pyyntö reseptitietokantaan
712
vastaanota vastaus
713
lähetä vastaus käyttäjälle
714

FIG 7